REPENSEZ VOS HABITUDES EN REGARD DE VOS MOTS DE PASSE DE MANIÈRE À PROTÉGER VOS COMPTES DES PIRATES INFORMATIQUES

Août 2020 ITSAP.30.036

Vous avez des comptes en ligne pour tout, des services gouvernementaux jusqu'au magasinage. Chaque fois que vous créez un nouveau compte, vous devez créer un nom d'utilisateur et un mot de passe. Réutiliser ces justificatifs d'identités (c.-à-d., un nom d'utilisateur ou un courriel et un mot de passe) pour plusieurs comptes peut être pratique, mais vous facilitez ainsi la tâche pour un pirate informatique d'obtenir un accès à vos comptes et à vos renseignements personnels. La seule chose dont il a besoin est d'un mot de passe et il a ensuite la clé pour tous vos comptes.

RÉUTILISER UN MOT DE PASSE VOUS MET À RISQUE

Les justificatifs d'identité d'utilisateurs sont de grande valeur pour les pirates informatiques parce qu'ils savent que les gens ont tendance à réutiliser leurs mots de passe plus d'une fois. Mais, comment font-ils pour obtenir votre mot de passe? Les pirates informatiques ciblent des organismes et des personnes, profitent des vulnérabilités de systèmes et de logiciels, envoient des courriels d'hameçonnage, camouflent des maliciels en les faisant passer pour des fichiers légitimes, tout ça dans le but d'obtenir de l'information sensible comme les justificatifs d'identité d'utilisateurs. Une fois qu'ils ont cette information, les pirates informatiques peuvent la vendre ou la publier en ligne, la mettant ainsi à disposition d'autres pirates. Vous utilisez peut-être encore aujourd'hui un mot de passe qui a été volé il y a des années, ceci vous met à risque d'être la victime de cyberattaques comme le **bourrage d'identifiants**. Pour vous protéger, évitez de réutiliser un mot de passe, même si vous le jugez complexe et difficile à deviner.

LE BOURRAGE D'IDENTIFIANTS

Dans le cas d'une attaque par bourrage d'identifiants, les pirates informatiques utilisent des justificatifs d'identité précédemment volés (c.-à-d., votre nom d'utilisateur ou votre courriel et votre mot de passe) d'un site Web en particulier et « bourrent » les pages de connexion d'autres sites Web ou systèmes jusqu'à ce qu'ils trouvent des correspondances. Les pirates informatiques utilisent des outils comme des réseaux de zombies, un ensemble de robots internet ou de dispositifs connectés sur Internet, et des applications pour tenter d'établir des correspondances entre des justificatifs d'identité et des comptes automatisant ainsi les attaques afin de mettre à l'essai les justificatifs sur plusieurs sites Web. Une fois qu'un pirate obtient un accès à un de vos comptes, il peut changer votre mot de passe, voler tous les renseignements de la carte de crédit qui y est associée et effectuer des transactions non autorisées ou mener d'autres activités frauduleuses.

HABITUDES À ADOPTER EN REGARD DE VOS MOTS DE PASSE

Le mot de passe est la première ligne de défense de vos comptes. Suivez les conseils ci-dessous pour les rendre efficaces :

- Utilisez une phrase de passe ou un mot de passe unique pour chacun de vos comptes.
- Activez l'authentification à facteurs multiples (AFM) de vos comptes lorsque c'est possible. L'AFM ajoute une couche de protection en demandant de prouver votre identité de plusieurs façons lorsque vous vous connectez à votre compte (p. ex., en fournissant un code de sécurité ou des identificateurs biométriques). Pour des instructions sur le paramétrage de l'AFM pour des services populaires en ligne, consultez le site : www.telesign.com/turnon2fa/tutorials
- Utilisez un gestionnaire de mots de passe (application autonome ou par navigateur) pour vous aider à vous rappeler vos mots ou phrases de passe uniques. Assurez-vous d'utiliser un mot de passe principal qui est robuste et d'activer l'AFM de votre gestionnaire de mots de passe.

ÉTAPES À SUIVRE SI VOTRE COMPTE EST COMPROMIS

Si vous soupçonnez que votre compte a été compromis, suivez les étapes suivantes pour vous protéger :

1. Changez immédiatement votre phrase ou mot de passe. Si vous avez réutilisé ce mot de passe pour d'autres comptes, assurez-vous de changer les mots de passe de ces comptes.
2. Vérifiez attentivement l'information de votre compte. Assurez-vous qu'aucun changement non autorisé n'a été apporté. Si c'est le cas, changez vos questions et réponses de sécurité.
3. Vérifiez qu'aucune activité suspecte n'ait été menée avec votre carte de crédit ou à vos comptes bancaires. Si votre carte de crédit est liée à un compte compromis, communiquez avec votre banque.
4. Communiquez avec le Centre antifraude du Canada (www.antifraudcentre-centreantifraude.ca) et avec la police locale si vous suspectez des activités frauduleuses et si vous vous inquiétez d'un vol d'identité. Vous voudriez peut-être également communiquer avec un bureau de crédit.

Visitez le site Web du Centre pour la cybersécurité (cyber.gc.ca) pour trouver des publications à ce sujet : *ITSAP.30.032 Pratiques exemplaires de création de phrases de passe et de mots de passe*, *ITSAP.30.030 Sécurisez vos comptes et vos appareils avec une authentification multifacteur*, et *ITSAP.30.025 Conseils de sécurité sur les gestionnaires de mots de passe.*

SÉRIE SENSIBILISATION